# Cassandra Crossing 620/ Spagna: prove generali di apocalisse?

(620)—Il blackout spagnolo ha fatto breccia nelle news, e forse ha anche spaventato qualcuno. Ma non abbastanza. E la cosa più…

---

**Cassandra Crossing 620/ Spagna: prove generali di apocalisse?**




Figure 1: Dr. Strangelove trailer from 40th Anniversary Special Edition DVD, 2004. This work is in the public domain in United States because it was published in United States between 1929 and 1977, without a copyright notice.

*(620)—Il blackout spagnolo ha fatto breccia nelle news, e forse ha anche spaventato qualcuno. Ma non abbastanza. E la cosa più importante non è stata mai nemmeno accennata.*

**5 maggio 2025**—Per parlare del recente blackout iberico, anzi multinazionale, Cassandra oggi partirà dalla fine, esponendo la sua profezia e poi cercando di spiegarla. Essendo Cassandra una profetessa di sventura, perdipiù mai creduta, poteva esordire diversamente?

**Il blackout spagnolo**, se non è stato un semplice incidente che ha buttato giù una rete troppo fragile, **è stato un test**, forse un atto dimostrativo, insomma una prova muscolare di un attacco cibernetico, **di una futura guerra multidimensionale**.

Un test cibernetico in scala reale, come i buoni, vecchi test nucleari di una volta. Nessuna (o pochissime) vittime, una prova di buon funzionamento di una nuova arma, e magari un messaggio per chi "*deve capire*".

Ora lo spiegone, più che altro in termini di "*Io l'avevo detto!*".

E come sempre è necessario riavvolgere il nastro e fare una breve introduzione storica. Scusate ancora una volta la vostra profetessa preferita.

I 24 indefessi lettori ricorderanno certamente che in più occasioni, Cassandra aveva esternato (1, 2, 3, 4) che da anni sono già in atto "test su strada" di armi cibernetiche.

Il più antico, che sia emerso agli onori delle cronache informatiche dell'epoca, risale al 2003, quello di SQL Slammer.

Si trattò di un malware autoreplicante, del tipo residente solo in memoria, che utilizzava una falla (CVE-2002–0649) di Microsoft SQL server, all'epoca un database molto diffuso sia su internet che in ambito aziendale.

Questo malware non eseguiva nessuna azione dannosa, né tentava di installarsi sui server che contagiava. Si limitava a cercare con estrema insistenza altri server da contagiare, inviando un semplice pacchetto UDP di soli 376 byte sulla porta 1434 di qualsiasi macchina che individuasse.

In questo modo, senza commettere nessuna azione distruttiva, saturava la connessione al server, provocando un DOS, un attacco di negazione del servizio sul database, ed a cascata anche sulla connessione di rete del server stesso e sui router che la gestivano.

Con estrema efficacia e rapidità, in soli 10 minuti SQL Slammer mandò fuori servizio buona parte dei database del mondo, provocando la caduta di innumerevoli servizi ed un rallentamento generalizzato dell'intera Internet di allora.

Vale la pena di dedicare giusto un rigo per sottolineare che il bug era noto da più di un anno, che Microsoft aveva rilasciato la patch sei mesi prima, e che quasi nessuno (anche in Microsoft) l'aveva applicata. E che il fatto di parlarne pubblicamente o nascondere il più possibile i fatti era già allora un ricorrente oggetto di dibattito.

La cura per SQL Slammer? Semplicissima, filtrare la porta UDP 1434, poi spegnere e riaccendere ogni server per cancellare il malware ed infine applicare la patch.

Distruzione totale dell'obbiettivo ma nessun danno permanente, oltre ai costi degli enormi disservizi creati. Come il test di una perfetta testata nucleare "pulita".

La ripetizione di questo semplice esempio, che annoierà alcuni ormai stanchi di rileggerlo, era necessaria, ma per fortuna siamo arrivati alla fine.

Da allora Internet è diventata sempre più grande ed enormemente più complessa. Qualsiasi oggetto remoto che avesse bisogno di essere monitorato, a cominciare dai tralicci degli elettrodotti, vi è stato connesso alla bell'è meglio, senza nessuna considerazione di sicurezza o resilienza, ma al solo fine di automatizzare e risparmiare.

Poi, quando dieci o venti anni dopo i nodi hanno iniziato a venire al pettine, se ne è cominciato a parlare. E parlare. E parlarne ancora.

Ma intanto l'intera rete elettrica e tutte le altre reti di distribuzione che tengono in piedi il mondo, e garantiscono (più o meno) la sopravvivenza di nove miliardi di esseri umani, sono piene di software, connessioni e protocolli che da una parte sono indispensabili e non si possono toccare, dall'altra andrebbero rifatti da zero, riprogettando tutto in sicurezza, e sopratutto eseguendo approfonditi e specifici test di resilienza.

E siamo arrivati ad oggi.

In questo mondo di infrastrutture colabrodo, che spesso stanno su non si sa bene come, arrivano i ciberguerrieri, prima come gruppetti anonimi altamente competenti e ben finanziati da stati nazionali ed altri attori, poi come armate ufficiali di eserciti multidimensionali.

Secondo voi, che cosa hanno fatto tutti questi signori negli ultimi dieci o venti anni? Sono stati solo alle fiere di sicurezza informatica a partecipare ai capture-the-flag?

Od hanno piuttosto cominciato ad infiltrarsi silenziosamente in giro, acquisendo competenze e mappando le vulnerabilità del "territorio cibernetico" di tutto il mondo, realizzando e testando armi cibernetiche, ma soprattutto piani di attacco, come fa da sempre qualsiasi organizzazione militare?

E durante queste attività, non gli sarà mai scappato il dito sul grilletto?

Non avranno mai avuto bisogno di fare qualche "prova su strada" che non costituisse un atto di guerra?

Non avranno mai dovuto mandare "messaggi" a chi doveva capire?

Non avranno mai utilizzato localmente una singola arma per combattere una delle tante guerre non dichiarate?

C'è ancora qualcuno a cui il nome "Stuxnet" non fa venire in mente nulla?

Che prove ha Cassandra di tutto ciò? Ovviamente nessuna, altrimenti farebbe, come tanti altri competentissimi ex-attori della scena hacker italiana, il consulente di security od il professore universitario.

Od almeno, nessuna "prova" che non sia già abbondantemente apparsa sulle news od in letteratura tecnica.

Fa solo il suo mestiere di profetessa, ragionando senza timore su ciò che tutti sanno, senza andarlo a chiedere ad una falsa intelligenza artificiale od agli addetti stampa di potenti organizzazioni.

E, anche mentre scrive, sempre sperando di sbagliare.

---

Scrivere a Cassandra—Twitter—Mastodon
Videorubrica "Quattro chiacchiere con Cassandra"
Lo Slog (Static Blog) di Cassandra
L'archivio di Cassandra: scuola, formazione e pensiero

***Licenza d'utilizzo**: i contenuti di questo articolo, sono sotto licenza Creative Commons Attribuzione—Condividi allo stesso modo 4.0 Internazionale (CC BY-SA 4.0),* tutte le informazioni di utilizzo del materiale sono disponibili a questo link.

By Marco A. L. Calamari on May 10, 2025.

Canonical link

Exported from Medium on August 27, 2025.